Boletín de alerta

Boletín Nro.: 105
Fecha de publicación: 18/12/2025
Tema: Alerta 2025-105 Vulnerabilidad ZeroDay en dispositivos SMA 100 siendo explotada activamente.
Traffic Light Protocol (TLP): White

Producto(s) afectado(s):

Secure Mobile Access (SMA) 1000:

- 12.4.3-03093 (platform-hotfix) y versiones anteriores.
- 12.5.0-02002 (platform-hotfix) y versiones anteriores.

Nota: Esta vulnerabilidad no afecta a SSL-VPN que se ejecuta en firewalls SonicWall.

Descripción

Se ha reportado la explotación activa de una vulnerabilidad de escalada de privilegios locales debido a una autorización insuficiente en la consola de administración del dispositivo SonicWall SMA1000 (AMC). Se ha identificado con el CVE-2025-40602 con un CVSSv3 6.6.

Se informó que esta vulnerabilidad se aprovechaba en combinación con CVE-2025-23006 (puntuación CVSS 9.8) para lograr la ejecución remota de código (RCE) no autenticado con privilegios de root. CVE-2025-23006 se corrigió en enero de 2025. Si desea mas información sobre esta ultima puede dirigirse al siguiente aqui.

Las únicas rutas de explotación conocidas para CVE-2025-40602 (CVSS 6.6) requieren que CVE-2025-23006 (CVSS 9.8) permanezca sin parchear o que el actor de amenazas ya posea acceso a una cuenta del sistema local. Si CVE-2025-23006 no se ha parcheado, el sistema ya está expuesto a una vulnerabilidad crítica. En este escenario, la aplicación de CVE-2025-40602 no aumenta significativamente el riesgo general ni la superficie de ataque.

La Agencia de Seguridad de Infraestructura y Ciberseguridad de Estados Unidos (CISA) ha agregado CVE-2025-40602 a su catálogo de Vulnerabilidades Explotadas Conocidas (KEV), requiriendo que las agencias de la Rama Ejecutiva Civil Federal (FCEB) apliquen las correcciones antes del 24 de diciembre de 2025 para proteger sus redes.

Solución:

El fabricante ha publicado actualización de seguridad en las versiones:

- 12.4.3-03245 (platform-hotfix) y versiones superiores.
- 12.5.0-02283 (platform-hotfix) y versiones superiores.

Puede redirigir al siguiente enlace para proceder con la actualización:

mysonicwall.com

Mitigación temporal:

Si aún no puede planear la actualización y/o la aplicación del parche de seguridad en su dispositivo, puede restringir el acceso a la consola de administración de dispositivos (AMC):

- Acceso SSH solo a través de VPN o direcciones IP de administrador específicas.
- Deshabilite la interfaz de administración de VPN SSL (AMC) y el acceso SSH desde Internet público.

Información adicional:

- **https://psirt.global.sonicwall.com/vuln-detail/SNWLID-2025-0019**
- **https://thehackernews.com/2025/12/sonicwall-fixes-actively-exploited-cve.html**
- https://www.tenable.com/blog/cve-2025-23006-sonicwall-secure-mobile-access-sma-1000-zero-day-reportedly-exploited